

LISTING OF CLAIMS:

Claim 1 (currently amended) A ~~remotely accessible~~ secure cryptographic system for storing a plurality of private cryptographic keys to be associated with multiple users, wherein said secure cryptographic system associates each of said multiple users with one or more different keys from said plurality of private cryptographic keys and performs cryptographic functions for each user using the associated one or more different keys without releasing said plurality of private cryptographic keys to said users, ~~[[the]]~~ said secure cryptographic system comprising:

a depository system having at least one server which stores a plurality of private cryptographic keys and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users and each of said multiple users is associated with one or more different keys from said plurality of private cryptographic keys;

an authentication engine which compares authentication data received by one of said multiple users to enrollment authentication data corresponding to said one of multiple users and received from said depository system, thereby producing an authentication result;

a cryptographic engine which, when said authentication result indicates proper identification of said one of the multiple users, performs cryptographic functions on behalf of the one of said multiple users using the associated one or more different keys received from said depository system; ~~[[and]]~~

a transaction engine connected to route data from the multiple users to said depository server system, said authentication engine, and said cryptographic engine; and

wherein said secure cryptographic system is remotely accessible.

Claim 2 (currently amended) A ~~remotely accessible~~ secure cryptographic system, comprising:

a depository system having at least one server which stores at least one private key and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users;

an authentication engine which compares authentication data received by one of said multiple users to enrollment authentication data corresponding to said one of multiple users and received from said depository system, thereby producing an authentication result;

a cryptographic engine which, when said authentication result indicates proper identification of said one of said multiple users, performs cryptographic functions on behalf of said one of said multiple users using at least said private key received from said depository system; ~~[[and]]~~

a transaction engine connected to route data from said multiple users to said depository server system, said authentication engine, and said cryptographic engine; and wherein said secure cryptographic system is remotely accessible.

Claim 3 (currently amended) The secure cryptographic system of Claim 2, wherein said depository system further comprises a plurality of data storage facilities, each data storage facility having at least one server storing a substantially randomized portion of said private key and a substantially randomized portion of said plurality of enrollment authentication data.

Claim 4 (currently amended) The secure cryptographic system of Claim 3, wherein each substantially randomized portion is individually undecipherable.

Claim 5 (currently amended) The secure cryptographic system of Claim 2, wherein said enrollment authentication data includes biometric data.

Claim 6 (currently amended) The secure cryptographic system of Claim 5, wherein said biometric data includes finger print patterns.

Claim 7 (currently amended) The secure cryptographic system of Claim 2, wherein said at least one private key corresponds to said secure cryptographic system.

Claim 8 (currently amended) The secure cryptographic system of Claim 2, wherein said at least one private key corresponds to said one of said multiple users.

Claim 9 (currently amended) The secure cryptographic system of Claim 2, wherein said cryptographic functions comprise one of digital signing, encryption, and decryption.

Claim 10 (previously presented) A method of facilitating cryptographic functions, said method comprising:

- associating a user from multiple users with one or more keys from a plurality of private cryptographic keys stored on a secure server;
- receiving authentication data from said user;
- comparing said authentication data to authentication data corresponding to said user, thereby verifying the identity of said user; and
- utilizing said one or more keys from a plurality of private cryptographic keys to perform cryptographic functions without releasing said one or more keys from a plurality of private cryptographic keys to said user.

Claim 11 (previously presented) The method of Claim 10, wherein said authentication data corresponding to said user was acquired prior to the step of receiving authentication data from said user.

Claim 12 (original) The method of Claim 10, further comprising receiving a hash of a message or document.

Claim 13 (previously presented) The method of Claim 12, further comprising archiving said hash.

Claim 14 (currently amended) An authentication system for uniquely identifying a user through secure storage of said user's enrollment authentication data, said authentication system comprising:

a plurality of data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores one of substantially randomized data portions of at least one piece of enrollment authorization data from enrollment authentication data; and

an authentication engine which communicates with said plurality of data storage facilities and comprises

a data splitting module which operates on said enrollment authentication data to create said substantially randomized data portions from said at least one piece of enrollment authorization data,

a data assembling module which processes ~~the~~ said substantially randomized data portions from at least two of said data storage facilities to assemble said at least one piece of enrollment authorization data from said enrollment authentication data, and

a data comparator module which receives current authentication data from a user and compares the current authentication data with the said assembled enrollment authentication data to determine whether said user has been uniquely identified.

Claim 15 (currently amended) The authentication system of Claim 14, wherein said substantially randomized data portions are not individually decipherable.

Claim 16 (previously presented) The authentication system of Claim 14, wherein said each data storage facility is logically separated from any other data storage facility.

Claim 17 (previously presented) The authentication system of Claim 14, wherein said each data storage facility is physically separated from any other data storage facility.

Claim 18 (previously presented) The authentication system of Claim 14, further comprising a cryptographic engine which, upon the unique identification of said user by said authentication engine, provides cryptographic functionality to said user.

Claim 19 (previously presented) The authentication system of Claim 14, wherein said plurality of data storage facilities comprises at least one secure server.

Claim 20 (previously presented) The authentication system of Claim 14, wherein unique identification of said user by said authentication engine provides said user authorization to gain access to or to operate one or more systems.

Claim 21 (previously presented) The authentication system of Claim 20, wherein said one or more systems include one or more electronic devices.

Claim 22 (previously presented) The authentication system of Claim 20, wherein said one or more systems include one or more computer software systems.

Claim 23 (previously presented) The authentication system of Claim 20, wherein said one or more systems include one or more consumer electronics.

Claim 24 (previously presented) The authentication system of Claim 23, wherein said one or more consumer electronics includes a cellular phone.

Claim 25 (previously presented) The authentication system of Claim 20, wherein said one or more systems include one or more cryptographic systems.

Claim 26 (previously presented) The authentication system of Claim 20, wherein said one or more systems include one or more physical locations.

Claim 27 (previously presented) The authentication system of Claim 14, wherein at least one of said data storage facilities stores at least some of sensitive data, wherein said at least one of said data storage facilities serves said sensitive data when said authentication engine indicates that said user has been uniquely identified.

Claim 28 (previously presented) The authentication system of Claim 14, further comprising a data vault which stores sensitive data, wherein said data vault serves said sensitive data when said authentication engine indicates that said user has been uniquely identified.

Claim 29 (previously presented) The authentication system of Claim 14, wherein said authentication system engine outputs an indication of whether said user has been uniquely identified.

Claim 30 (currently amended) A cryptographic system, comprising:

a plurality of data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores one of substantially randomized data portions of at least one cryptographic key[[s]] from a plurality of cryptographic keys; and

a cryptographic engine which communicates with said plurality of data storage facilities and comprises:

a data splitting module which operates on said cryptographic keys to create said substantially randomized data portions of at least one cryptographic key.

a data assembling module which processes the substantially randomized data portions from at least two of said data storage facilities to assemble said at least one cryptographic key[[s]] from said plurality of cryptographic keys, and

a cryptographic handling module which receives said assembled cryptographic keys and performs cryptographic functions therewith.

Claim 31 (currently amended) The cryptographic system of Claim 30, wherein said substantially randomized data portions are not individually decipherable.

Claim 32 (previously presented) The cryptographic system of Claim 30, wherein said each data storage facility is logically separated from any other data storage facility.

Claim 33 (previously presented) The cryptographic system of Claim 30, wherein said each data storage facility is physically separated from any other data storage facility.

Claim 34 (previously presented) The cryptographic system of Claim 30, further comprising an authentication engine which, before the cryptographic functionality may be employed on behalf of a user, uniquely identifies said user.

Claim 35 (previously presented) The cryptographic system of Claim 30, wherein said plurality of data storage facilities comprises at least one secure server.

Claim 36 (previously presented) A method of storing authentication data in geographically remote secure data storage facilities thereby protecting said authentication data against compromise of any individual data storage facility, said method comprising:

- receiving authentication data at a trust engine;

- combining at said trust engine said authentication data with a first substantially random value to form a first combined value;

- combining said authentication data with a second substantially random value to form a second combined value;

- creating a first pairing of said first substantially random value with said second combined value;

- creating a second pairing of said first substantially random value with said second substantially random value;

- storing said first pairing in a first secure data storage facility; and

- storing said second pairing in a second secure data storage facility remote from said first secure data storage facility.

Claim 37 (previously presented) A method of storing authentication data comprising:

- receiving authentication data;

combining said authentication data with a first set of bits to form a second set of bits;
combining said authentication data with a third set of bits to form a fourth set of bits;
creating a first pairing of said first set of bits with said third set of bits;
creating a second pairing of said first set of bits with said fourth set of bits;
storing one of said first and second pairings in a first computer accessible storage medium; and

storing the other of said first and second pairings in a second computer accessible storage medium.

Claim 38 (previously presented) The method of Claim 37, wherein at least one of said first and second computer accessible storage mediums comprises at least one server.

Claim 39 (previously presented) The method of Claim 37, wherein said first computer accessible storage medium is geographically remote from said second computer accessible storage medium.

Claim 40 (previously presented) The method of Claim 37, wherein the matching of one of said first and second pairings with one of said first and second computer accessible storage mediums is substantially random.

Claim 41 (previously presented) The method of Claim 37, wherein at least one of said first and third sets of bits are substantially random.

Claim 42 (currently amended) The method of Claim 37, wherein at least one of said first and third sets of bits comprises a bit length equal to a bit length of said authentication sensitive data.

Claim 43 (previously presented) The method of Claim 37, wherein both said first and second pairings are needed to reassemble said data.

Claim 44 (previously presented) The method of Claim 37, further comprising:

creating a third pairing of said second set of bits with said third set of bits;
creating a fourth pairing of said second set of bits with said fourth set of bits;
storing one of said third and fourth pairings in a third computer accessible storage medium; and

storing the other of said third and fourth pairings in a fourth computer accessible storage medium.

Claim 45 (previously presented) A method of storing cryptographic data in geographically remote secure data storage facilities thereby protecting said cryptographic data against compromise of any individual data storage facility, said method comprising:

receiving cryptographic data at a trust engine;
combining at said trust engine said cryptographic data with a first substantially random value to form a first combined value;
combining said cryptographic data with a second substantially random value to form a second combined value;
creating a first pairing of said first substantially random value with said second combined value;
creating a second pairing of said first substantially random value with said second substantially random value;
storing said first pairing in a first secure data storage facility; and
storing said second pairing in a secure second data storage facility remote from said first secure data storage facility.

Claim 46 (currently amended) A method of storing cryptographic data comprising:

receiving cryptographic authentication data;
combining said cryptographic data with a first set of bits to form a second set of bits;
combining said cryptographic data with a third set of bits to form a fourth set of bits;
creating a first pairing of said first set of bits with said third set of bits;
creating a second pairing of said first set of bits with said fourth set of bits;
storing one of said first and second pairings in a first computer accessible storage medium; and
storing the other of said first and second pairings in a second computer accessible storage medium.

Claim 47 (previously presented) The method of Claim 46, wherein at least one of said first and second computer accessible storage mediums comprises at least one server.

Claim 48 (previously presented) The method of Claim 46, wherein said first computer accessible storage medium is geographically remote from said second computer accessible storage medium.

Claim 49 (previously presented) The method of Claim 46, wherein the matching of one of said first and second pairings with one of said first and second computer accessible storage mediums is substantially random.

Claim 50 (previously presented) The method of Claim 46, wherein at least one of said first and third sets of bits are substantially random.

Claim 51 (currently amended) The method of Claim 46, wherein at least one of said first and third sets of bits comprises a bit length equal to a bit length of said cryptographic sensitive data.

Claim 52 (previously presented) The method of Claim 46, wherein both said first and second pairings are needed to reassemble said cryptographic data.

Claim 53 (previously presented) The method of Claim 46, further comprising:

creating a third pairing of said second set of bits with said third set of bits;

creating a fourth pairing of said second set of bits with said fourth set of bits;

storing one of said third and fourth pairings in a third computer accessible storage medium; and

storing the other of said third and fourth pairings in a fourth computer accessible storage medium.

Claim 54 (currently amended) A method of handling sensitive data from a plurality of users in a cryptographic system, wherein said sensitive data exists in a useable form only during actions employing said sensitive data, said method comprising:

receiving in a software module, substantially randomized sensitive data portions from a first computer accessible storage medium;

receiving in said software module, substantially randomized data portions from a second computer accessible storage medium,

processing said substantially randomized sensitive data portions and said substantially randomized data portions in said software module to assemble said sensitive data; and

employing said sensitive data in a software engine to authenticate exactly one of said plurality of users.

Claim 55 (previously presented) The method of Claim 54, further comprising destroying said sensitive data after completion of said action.

Claim 56 (previously presented) The method of Claim 54, wherein said sensitive data includes one of user biometric data and cryptographic key data.

Claim 57 (previously presented) The method of Claim 54, wherein at least one of said first and second computer accessible storage mediums comprise a secure server.

Claim 58 (previously presented) The method of Claim 54, wherein said software module comprises a data assembling module and said software engine comprises one of an authentication engine and a cryptographic engine.

Claim 59 (currently amended) A secure authentication system, comprising:

a plurality of authentication engines, wherein each authentication engine receives substantially randomized data portions of at least one piece of enrollment authentication data which once assembled are designed to uniquely identify a user to a degree of certainty, each authentication engine receives current authentication data to compare to said assembled enrollment authentication data, and wherein each authentication engine determines an authentication result; and

a redundancy system which receives said authentication result of at least two of said authentication engines and determines whether said user has been uniquely identified.

Claim 60 (previously presented) The secure authentication system of Claim 59, wherein said redundancy system determines whether said user has been uniquely identified by following the majority of said authentication results.

Claim 61 (previously presented) The secure authentication system of Claim 59, wherein said redundancy system determines whether said user has been uniquely identified by requiring said authentication results to be unanimously positive before issuing a positive identification.

Claim 62 (previously presented) The secure authentication system of Claim 59, wherein said redundancy system includes a plurality of redundancy modules, and said secure authentication system further comprises:

a plurality of geographically remote trust engines, each trust engine having one of said plurality of authentication engines and one of said redundancy modules,

wherein the redundancy module for at least one of said plurality of trust engines determines whether said user has been uniquely identified using said authentication results from ones of said authentication engines associated with the other trust engines and without using said authentication results from the at least one trust engine.

Claim 63 (currently amended) The secure authentication system of Claim 62, wherein each of said plurality of trust engines includes a depository having a computer accessible storage medium which stores said [[a]] substantially randomized data portions of at least one piece of said enrollment authentication data and wherein each depository forwards said substantially randomized data portions of said enrollment authentication data to said plurality of authentication engines.

Claim 64 (original) The secure authentication system of Claim 62, wherein said determination of whether said user has been uniquely identified corresponds to the one of said redundancy modules to first determine a result.

Claim 65 (currently amended) A trust engine system for facilitating authentication of a user, said trust engine system comprising:

a first trust engine comprising a first depository, wherein said first depository includes a computer accessible storage medium which stores substantially randomized data portions of at least one piece of enrollment authentication data from a plurality of enrollment authentication data;

a second trust engine located at a different geographic location than said first trust engine and comprising:

a second depository having a computer accessible storage medium which stores substantially randomized data portions of at least one piece of said enrollment authentication data,

an authentication engine communicating with said first and second depositories and which assembles at least two of said substantially randomized data portions of at least one piece of said enrollment authentication data into a usable form, and

a transaction engine communicating with said first and second depositories and said authentication engine,

wherein when said second trust engine is determined to be available to execute a transaction, said transaction engine receives enrollment authentication data from a user and forwards a request for substantially randomized data portions of at least one piece of enrollment authentication data to said first and second depositories, and wherein said authentication engine receives said enrollment authentication data from said transaction engine and the substantially randomized data portions of at least one piece of said enrollment authentication data from said first and second depositories, and determines an authentication result.

Claim 66 (previously presented) The trust engine system of Claim 65, wherein said determination of whether said second trust engine is available to execute said transaction includes a determination of whether said second trust engine is within geographic proximity to said user.

Claim 67 (previously presented) The trust engine system of Claim 65, wherein said determination of whether said second trust engine is available to execute said transaction includes a determination of whether said second trust engine is currently servicing a light system load.

Claim 68 (previously presented) The trust engine system of Claim 65, wherein said determination of whether said second trust engine is available to execute said transaction includes a determination of whether said second trust engine is currently scheduled for maintenance.

Claim 69 (previously presented) The trust engine system of Claim 65, wherein said first and second trust engines are determined to be available, and an authentication result for said trust engine system follows said first of said first and second trust engines to produce said authentication result.

Claim 70 (previously presented and currently amended) A method of handling sensitive data in a cryptographic system, wherein said sensitive data exists in a useable form only during actions employing said sensitive data, said method comprising:

- receiving in a software module, substantially randomized sensitive data portions from a first computer accessible storage medium;

- receiving in said software module, substantially randomized data portions from a second computer accessible storage medium,

- processing said substantially randomized sensitive data portions from said first computer accessible storage medium and said substantially randomized data portions from said second computer accessible storage medium in said software module to assemble said sensitive data; and

- employing said sensitive data in a software engine to perform a cryptographic function.

Claim 71 (previously presented) The method of Claim 70, further comprising destroying said sensitive data after completion of said action.

Claim 72 (previously presented) The method of Claim 70, wherein said sensitive data includes one of user biometric data and cryptographic key data.

Claim 73 (previously presented) The method of Claim 70, wherein at least one of said first and second computer accessible storage mediums comprise a secure server.

Claim 74 (previously presented) The method of Claim 70, wherein said software module comprises a data assembling module and said software engine comprises one of an authentication engine and a cryptographic engine.